OPEGA
REVIEW

FINAL REPORT

State-Wide Planning and Management of Information Technology

JANUARY
2006

a report by

the Office of Program Evaluation & Government Accountability

About the Review

Purpose

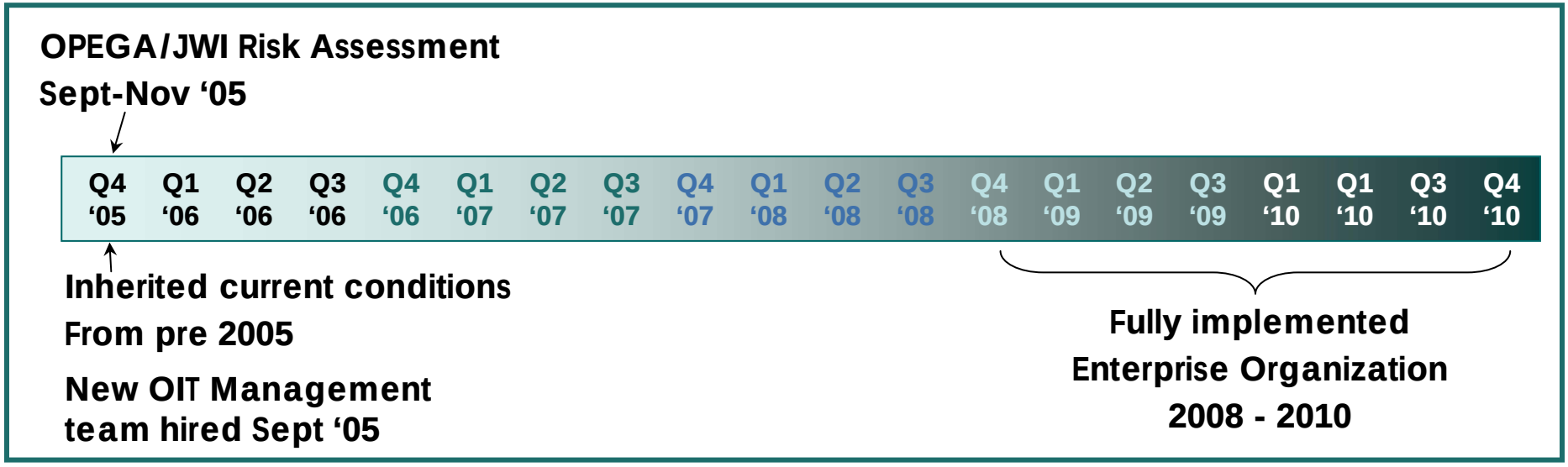
OPEGA Seeks to Answer the Question…

Is information technology (IT) being planned for and managed in a way that:

- maximizes the effectiveness and efficiency of State government; and
- keeps the State's exposure to associated risks at an acceptable level?

Purpose

OPEGA's review was performed during the initial phases of OIT Consolidation.



Methods

To answer this question, OPEGA …….

- Combined high level Best Practice evaluation with IT Risk Assessment
- Conducted research on:
  - State's history related to IT
  - Current organization and plans for IT
  - Role of IT in government
  - Models and best practices related to the planning and management of IT in government
- Partnered with contracted team of specialized IT auditors to conduct Risk Assessment

Methods

- Best Practice Models were those consistently identified by:
  - Federal GAO and OMB
  - NASCIO
  - Customer Management Community Forum
- OPEGA compared current State situation and plans to models
- Risk Assessment based on COBIT, an industry standard framework for IT risk management
- Risk Assessment took broad survey approach involving 31 State organizational units

What is a Risk Assessment?

Government/Quality Objectives

What are we trying to achieve?

Risks or Threats to Achievement

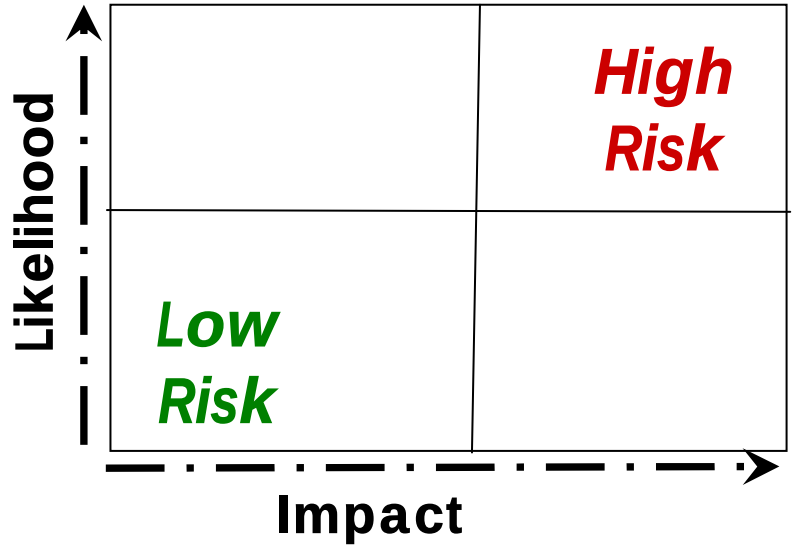
What could go wrong? How likely is it? What's the potential impact?

Controls

How do we prevent it, detect it or reduce its impact?

Exposure

What's the likelihood and impact with controls in place?



Is it Acceptable?

Risk Assessment Results

- ✓ JWI delivered a detailed report of their results to OPEGA in November 2005; report became part of OPEGA's working papers
- ✓ Deliverables from JWI included detailed Risk Matrix and recommended 3 year audit plan
- ✓ Details were shared with CIO & key staff; also shared with GOC as Interim Report
- ✓ Results were integrated with best practices evaluation to develop findings/observations for this report

Background

Role of IT in Government

- Like all other organizations, government has become reliant on IT
- IT has become a function or "program" that itself needs to be held accountable to public
- IT provides critical infrastructure that must be carefully developed, maintained and managed

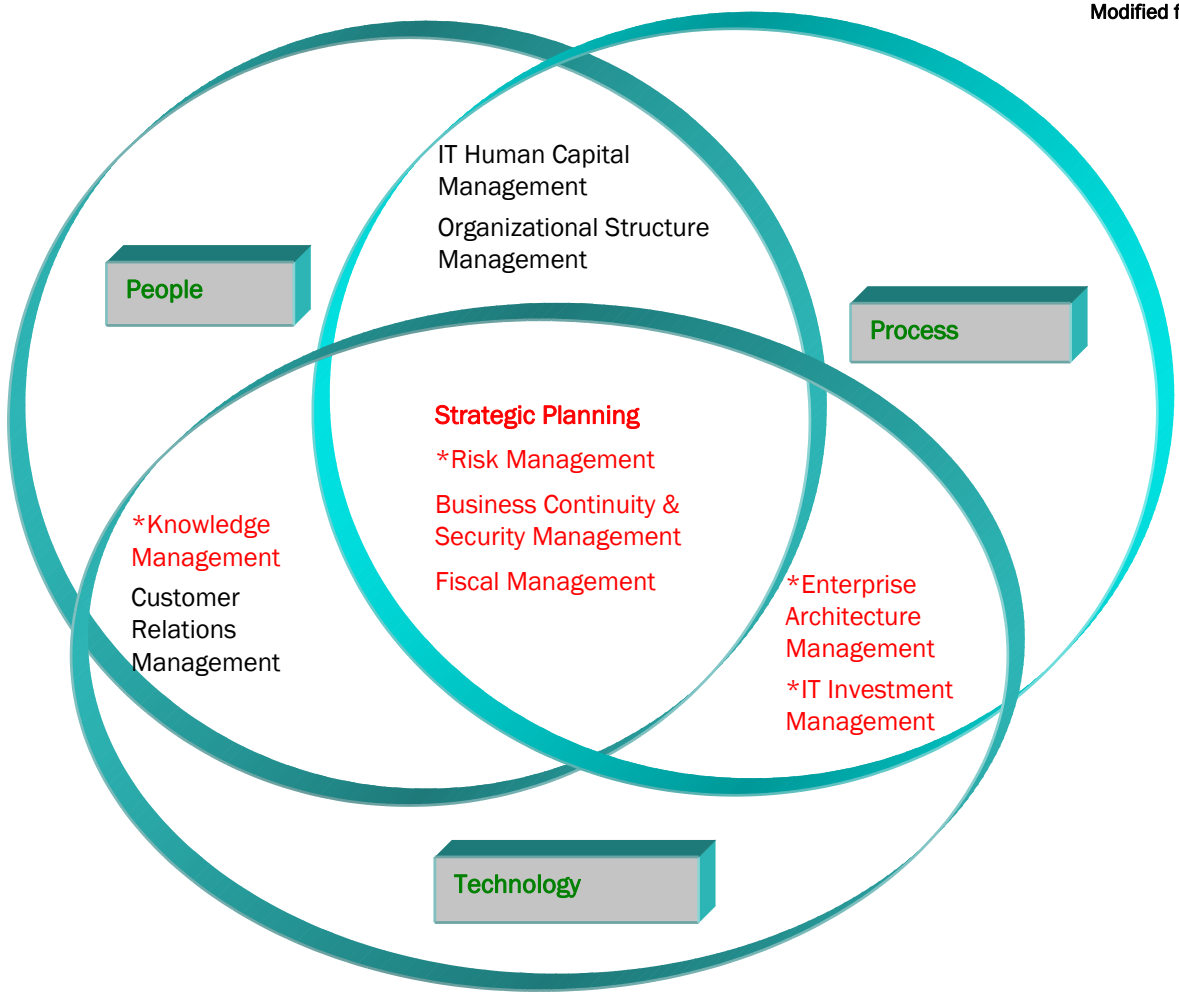
Best Practices in IT

Institutional practices, that bring together people, processes and technology to achieve goals, serve as high-level management controls to mitigate IT risks.

Maine's IT is immature in regard to many of these practices. *Best practice models for the most unfamiliar practices are discussed in report.

Figure 3. Relationship among Management Controls, People, Processes, and Technology

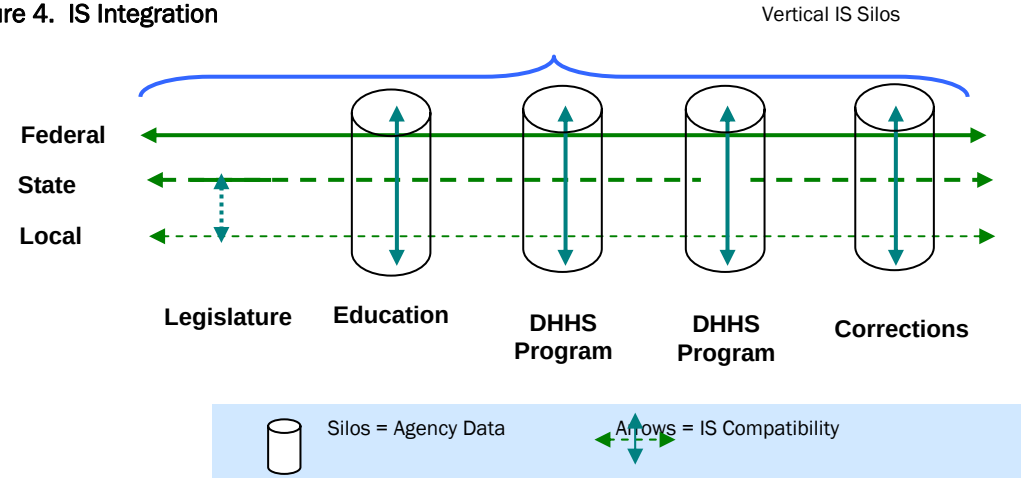
Modified from US GAO



Evolution of IT in Maine

- IT development in environment of rapid technology change; drastic changes in policy and mandates
- Federal government funding of IT goes directly to State agencies to support specific programs
- Impetus for vertical integration resulted in IT operations "silo-ed" in each State agency; IT resource decisions made at agency level

Figure 4. IS Integration



Evolution of IT in Maine

- Fragmented approach has resulted in:
  - Curtailed capacity to perform core state-level functions
  - Uncontrolled expenditure on uncoordinated contracts; lack of investment in IS infrastructure
  - Inefficiencies, duplication of efforts, and missed opportunities
- Fragmented approach with resource constraints has created IT culture of "operational expediency"

Evolution of IT in Maine

- Operational expediency has resulted in:
  - Lack of meaningful financial and management information
  - No enterprise-wide strategic planning for IT
  - Lack of standard, State-wide project management processes
  - Agencies constantly reacting to IT crises
  - Expensive retrofitting of new systems
  - Weak checks and balances in acquisitions and contract oversight
  - Employees hampered by out of date systems or problematic new ones

Evolution of IT in Maine

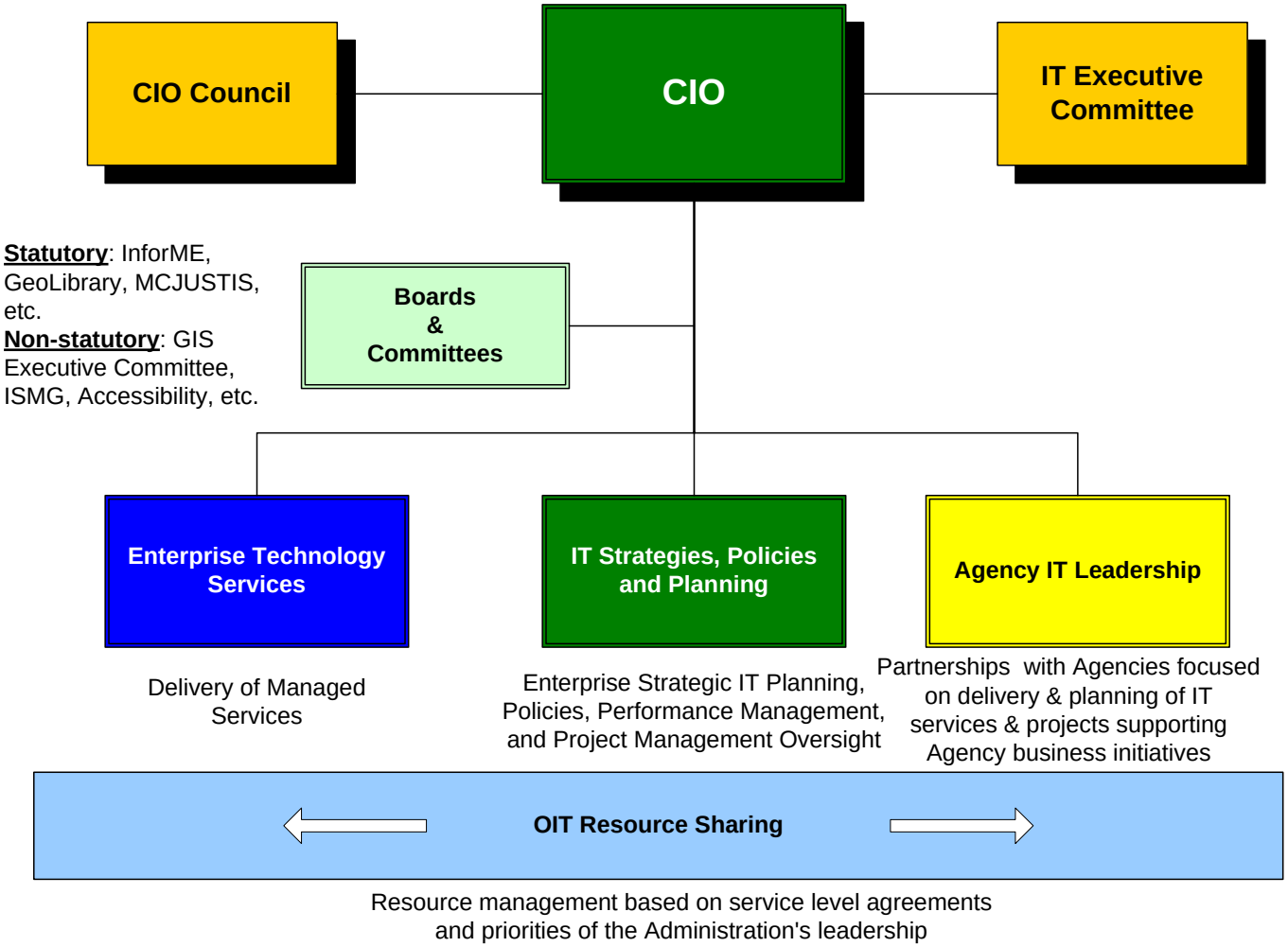
- Despite problems with fragmented approach, Maine has been slow to adopt "enterprise" approach to IT
- Attempts to coordinate or centralize some IT functions brought some successes but have not been far-reaching enough
- Planning for major transformation to enterprise approach finally commenced in 2003 with appointment of current CIO

Evolution of IT in Maine

- Real transformation began in 2005 with consolidation of Executive branch IT into the Office of Information Technology under CIO
- OIT consolidation:
  - integrates relatively independent IT "universes" that had varying resources and priorities
  - moves State toward IT structure that allows planning & managing from an "enterprise" perspective
- Expect 3-5 years before full benefits are realized.

OIT Organization

Office of Information Technology
Final Draft - June 16, 2005
Overall OIT Model



Conclusions

Conclusions

A. For some time now, State's historical approach to planning and managing IT has not been adequate to:

- Maximize effectiveness and efficiency
- Keeps risks to acceptable levels

Culture of operational expediency has put planning, risk management, sound policies and procedures on back burner

State is currently exposed to unacceptable level of IT-related risk

Conclusions

B. OIT consolidation is poised to significantly improve situation as it takes an enterprise approach to planning and management of IT across Executive branch

Some additional elements need to be added to OIT's Strategic Plan.

Enterprise does not currently include Judicial and Legislative branches.

Conclusions

C. Success of transformation efforts depends on CIO's capabilities and support from Executive and Legislative branches.

Related risks need to be monitored and managed by leaders in both branches.

Legislature has no real mechanism for supporting and overseeing enterprise-wide IT strategic plan and transformation

Findings and Observations

Enterprise Architecture Management

- an organizational blueprint that defines – in business and technology terms – how an organization operates today, how it intends to operate in the future and how it intends to get from here to there

  Maine is only beginning to develop EA to guide IT development.

  OPEGA has 3 findings/observations related to EAM

Finding 1

Finding

Descriptions of "as is" and "to be" environments have not yet been developed.

Management Action

OIT will create descriptions of "as is" and "to be" environments with all appropriate elements including sequencing steps.

CIO will provide regular update on progress to oversight and advisory bodies.

Finding 2

Finding

Written policies and procedures are either non-existent, inadequate or inconsistent across Executive branch in a number of IT areas.

Management Action

Standardized policies and procedures will be developed, communicated and implemented across the enterprise. High priority issues first; others as time and resources permit.

Observation 1

Observation

Enterprise approach is currently focused on Executive branch and does not include Judicial or Legislative branches; some improvement opportunities will not be realized.

Recommendations

A. Constitutional Officers and reps from Judicial and Legislative branch should actively participate on CIO Council

B. Judicial and Legislative branches should explore opportunities to contract with OIT

C. Legislature could establish specific group to manage EA and IT investment for whole state.

Investment Management

- selecting and controlling IT spending so as to maximize return on investment and minimize risk.

Maine does not treat information systems as major capital assets requiring disciplined investment management.

OPEGA has 2 findings related to IM

Finding 3

Finding

Current accounting structures and financial practices do not provide view of IT budgets and expenditures across the State as a whole, or by any specific activity, program or statute.

Management Actions

1. CIO will study feasibility of establishing IT as a "program"
2. CIO will initiate effort to modify account code structures
3. OIT is developing rate structure to reflect actual costs

Recommendation

Judicial and Legislative branches should explore establishing IT as "program"

Finding 4

Finding

Decisions on IT investments have not been made from an enterprise perspective or by a centralized State entity.

Management Actions

1. OIT's enterprise architecture will guide IT investments
2. Proposed or requested capital investments in IT will be reviewed and approved by OIT's Project Review Committee

Risk Management

- addressing potential events or situations that threaten the successful achievement of organizational objectives

Maine has not employed risk management approach in making IT decisions.

OPEGA has 1 finding related to RM

Finding 5

Finding

Risk assessment found 1% of IT environment highly controlled; 11% satisfactorily controlled and 88% with undesirable level of control. State is exposed to unacceptable level of IT-related risk.

Specific exposures addressed in other findings and observations. Overall results indicate need for risk management process.

Management Action

OIT will construct risk management plan that builds on risk assessment results and works to mitigate priority risks. Plan will include on-going audit and review of risk on specific projects.

Recommendation

OPEGA should establish schedule of IT review to include in future work plans.

Project Management

Weak or inconsistent project management has been recurring root cause of problems for system implementation projects. OIT has created formal Project Management Office to improve quality and depth of State's project management capabilities.

OPEGA has 2 findings related to PM

Finding 6

Finding

There has been little effort to ensure that individuals managing IT projects, whether State staff or vendors, have strong project management capabilities.

Management Actions

1. OIT staff will be educated in PM and will support agencies
2. OIT will establish policy/procedures requiring agencies to engage OIT PMO before formulating system solutions
3. OIT now has responsibility for contracting with vendors on IT projects and will consider PM capabilities during vendor selection

Finding 7

Finding

State of Maine lacks effective System Development Life Cycle (SDLC) process and attendant project management methodology.

Management Action

OIT Project Management Office has adopted Ten Step PM methodology and will be adopting a SDLC methodology

Security and Business Continuity

Security controls reduce risk of loss or damage to IT assets. Business continuity plans assure continued operations if loss or damage actually occurs.

OPEGA has 3 findings related to these areas

Finding 8

Finding

Risk assessment identified weaknesses in physical access security controls, particularly in regard to State's primary data center.

Management Actions

OIT Security Officer has developed action plan to address physical access security weaknesses in order of priority according to risk associated with each. Action plan was submitted to OPEGA on January 9, 2006.

Detailed actions are described in OPEGA report.

Finding 9

Finding

System access controls do not measure up to industry standards. Procedures are inadequate or inconsistently applied across enterprise; firewall rules are not well documented.

Management Actions

1. New IT Security Policy will clarify that established password policies and procedures apply to whole Executive branch
2. Plans are being developed to ensure password policies are enforced and passwords are encrypted
3. Independent audit of firewall rules is planned and should produce improved documentation

Finding 10

Finding

Business Continuity Planning is inadequate across Executive branch; State's ability to continue to perform functions and provide services following loss or damage to IS infrastructure is at risk.

Management Action

OIT will facilitate BCP by:

- Consolidating data centers
- Assessing current plans
- Identifying weaknesses
- Recommending remedies

Significant financial and human resources required

Recommendation

Each agency in all branches of State government should also develop its own BCP

Knowledge Management

- Capturing, understanding, and using the collective body of information and intellect within an organization to accomplish its mission

Maine has not treated knowledge and the information that supports it as assets.

OPEGA has 5 observation related to KM

Observation 2

Observation

Inadequate attention has been given to designing information systems that create accountability and are themselves accountable.

Management Action

OIT will investigate using knowledge management concepts including:

- Designing systems to produce performance data on programs
- Using automated tools to monitor performance metrics for information systems

Recommendation

Legislative bodies responsible for oversight of information system implementations should take an interest in system design

Observation 3

Observation

Ability to combine data from different sources or systems across the enterprise is very limited. Same data is often duplicated in several systems.

Management Actions

1. OIT will develop data standards to begin codifying common data elements across multiple information systems
2. New systems will be evaluated for common data elements that can be shared or architected as a common resource rather than duplicated
3. OIT is investigating tools to assist in exchanging data between legacy systems

Observation 4

Observation

Professional development opportunities for IT staff have been limited by resource constraints thus limiting exposure to new ideas and technologies that could help keep Maine current.

Management Actions

OIT will facilitate professional development program to keep technical staff current and assure emerging trends are assimilated to support the business.

Observation 5

Observation

The wealth of accumulated knowledge possessed by OIT staff may be lost as they choose to retire or otherwise leave state employment.

Management Actions

Succession planning and knowledge transfer were considerations in hiring the initial OIT enterprise management team; this focus will extend throughout the enterprise

Observation 6

Observation

The State's IT is not yet being well utilized to share knowledge around particular topics.

Management Actions

OIT will work to increase use of technology for information sharing over time and as resources permit. OIT expects to:

- Investigate feasibility of appointing a Chief Knowledge Officer
- Advocate that Data Stewards and Product Managers be designated
- Continue to foster use of technology for sharing information whenever opportunities arise

Leadership and Oversight

One of most recognized reasons for success of transformation efforts so far is leadership of current CIO and Administration support. Changes in leadership create risk that transformation will be disrupted before transformation is fully mature.

OPEGA has 2 observations related to this risk

Observation 7

Observation

Political process creates risk that frequent short-term leadership changes will interfere with long-term strategic planning for IT. CIO may change as early as January 2007.

Management Action

CIO has initiated two pronged approach to mitigate risk of change in leadership:

- strengthen OIT management team
- create new, widely supported strategic plan

Recommendation

Legislature should further mitigate this risk through:

- active support and oversight
- OPEGA reviews
- legislation requiring CIO to have certain qualifications

Observation 8

Observation

Legislative oversight activities devoted exclusively to the State's information technology on an enterprise-wide basis are absent.

Recommendations

A. Legislature should support any actions taken to establish IT as a "program"

B. Legislature should assign responsibility for oversight of enterprise-wide IT to either:

- JS Committee on Utilities and Energy; OR
- JS Committee on State and Local Government

Questions?